Technology Audit

Security

CRYPTOMAThIC Ltd.
Cryptomathic Authenticator

Written by: Andy Kellett

Date: November 2005

Abstract

Cryptomathic Authenticator is an authentication server that has been designed by Cryptomathic specifically to meet the security protection and user authentication needs of the banking sector and its customers. The solution provides a platform for the delivery of strong two-factor authentication services, and in doing so is capable of supporting a variety of authentication approaches. These can include one-time password tokens, card-and-reader tokens (including MasterCard CAP / VISA), paper-based TAN lists, SMS-driven response codes, and static passwords. Banks and financial institutions across the globe were quick to see the benefits that could be gained from offering on-line, self-service, and phone-based access to their products and services. Unfortunately, over the last two years, on-line banking and associated retail facilities have been blighted by a well-publicised range of security problems including: Phishing, PC Trojans, Spyware, and man-in-the-middle attacks. Cryptomathic Authenticator provides the banking community with a server-based customer authentication system that has the ability to integrate with existing banking infrastructure systems and take responsibility for all customer authentication services. Thus far banks and other customer-facing institutions have had to accept the financial risks associated with on-line fraud. However, for those that are prepared to take up the challenge, Cryptomathic Authenticator has the potential to help them to fight back.

KEY FINDINGS

Key: ✓ Product Strength ✗ Product Weakness *i* Point of Information

✓	Provides the back office platform and infrastructure to support a wide range of two-factor authentication systems.	✓	Integrated solution, whose architecture and interfaces have been designed to minimise their effect on existing legacy systems.
✓	Highly-scalable solution supported by application-level clustering and fail-over capabilities.	✓	Strong authentication solution that has been designed specifically for the banking sector.
✓	Provides strong customer protection against a range of Phishing, Pharming, Trojan, and Spyware threats.	*i*	Microsoft SQL and Oracle databases are supported by the solution, as well as HSMs from nCipher and Eracom Technologies.
i	The main authentication server platform of choice is Microsoft Windows Sever 2003. It can also be ported to various UNIX platforms.	✗	Immature market. Until recently, key users in the banking sector have been slow to take up the two-factor authentication challenge.

LOOK AHEAD

Market adoption of two-factor authentication systems in banking is still at the early adopter stage, whereas the technology to deliver such services in enterprise environments has been available for some time. Cryptomathic has built an end-to-end authentication solution to enable the transfer of authentication technology from enterprise to banking environments. The system integrates with a wide range of front-end systems and utilises black-box HSM technology to add to the secure nature of its solution. Future enhancements will include further CAP integration of the product.

▶ FUNCTIONALITY

Without doubt the Internet has revolutionised the way that we all communicate. It has had a positive effect on both our business and private lives by changing our information access and delivery capabilities. Businesses worldwide were very quick to pick up on the fact that on-line customer self-service and phone-based customer-not-present trading activities, brought with them major cost-saving benefits. However, ease-of-use allied to a lack of forethought to the security implications by the early adopters of on-line trading has lead to a position where every on-line or telephone-based trading opportunity is now seen by fraudsters as an opportunity to make money. Spyware, Trojans, Phishing attacks, and other low-cost, spam-based threats have proliferated over the last two years, and because in the financial sector such attacks are targeted specifically towards gaining access to monetary assets they are damaging the ability of banking and financial services organisations to trade over the Internet.

Butler Group believes that a stage has now been reached where customers are becoming more reluctant to use on-line banking unless service providers are able to prove the secure nature of their facilities. Recent research, from a well-respected source, estimated that last year alone over 600,000 UK Internet users refused to use on-line banking services due to security fears. However, so far most financial losses that customers have suffered as a result of electronic fraud have been underwritten by the banks, but as the levels of on-line transaction and identity fraud continue to grow (last year's numbers in the UK alone exceeded UK£12 million), positive and effective action is needed. Cryptomathic is putting forward its Authenticator solution as a strong, future proof approach to the delivery of secure on-line banking services.

Product Analysis

To date, there has been reluctance within the banking community to provide millions of on-line customers with better/stronger authentication credentials. This has been mainly due to roll-out costs and operational complexity considerations. However, Butler Group believes that the difficult balance between risk and cost is now shifting in favour of the use of stronger authentication techniques as business and private customers demand to be better protected.

Cryptomathic Authenticator is an authentication server-based solution that has been designed by Cryptomathic specifically for use within banking applications. The product's role is to provide strong two-factor authentication each time a business or private customer attempts to gain access to their banking services and perhaps also each time they undertake/authenticate a financial transaction. The actual range of front-end authentication tools that can be selected by a bank or financial institution, as being appropriate for the services that it provides, can be quite wide ranging. Typically they can include:

- Grid cards.
- MasterCard CAP.
- SMS.
- Static Passwords.
- TAN cards.
- Vasco Digipass.
- Visa dynamic passcode authentication.
- Other new modular architecture methods.

All of the above authentication options are supported within the Cryptomathic Authenticator solution, and all can be sustained within the solutions in-line authentication architecture without significant impact upon the way that a financial institution's own customer management systems operate.

The core components of the Cryptomathic Authenticator solution involve the use of one or more Cryptomathic Authentication servers and associated database repositories. Database repositories are used to hold encrypted token information that matches each customer's secure access credentials. Depending upon the size of the operation the Cryptomathic solution will involve the use of one or more authentication servers.

Each authentication server is attached to a Hardware Secure Module (HSM). HSMs are hardened black-box devices that are used to provide absolute protection for the information that they hold. Within the Cryptomathic Authenticator solution, HSMs are used to store the system's Master Keys, and all requests that are handled by the Cryptomathic Authenticator's databases are then processed and authenticated by the HSM.

Each authentication server, associated databases, and HSM facilities have been designed to operate in-line but at the same time, independently of the bank's own customer management systems. They deliver integration with those systems, but at the same time provide their services with minimal impact upon the existing infrastructure. In addition, as Cryptomathic Authenticator is installed as a key component of a bank's live customer management infrastructure, the solution provides strong application level fail-over and clustering facilities that support high levels of redundancy and systems scalability (up to 10,000,000 users). In operational use servers can be added or removed from a configuration in real-time without impacting on the availability of services provided.

Product Operation

At its simplest level, Cryptomathic Authenticator is a Yes/No, user access, authentication solution. In operational use, and as shown in Figure 1 below, customers can use a range of authentication credentials to identify themselves and request real-time access to their bank account details and financial services facilities. The role of Cryptomathic's Authenticator solution is to allow or deny access to those facilities based on the credentials presented.

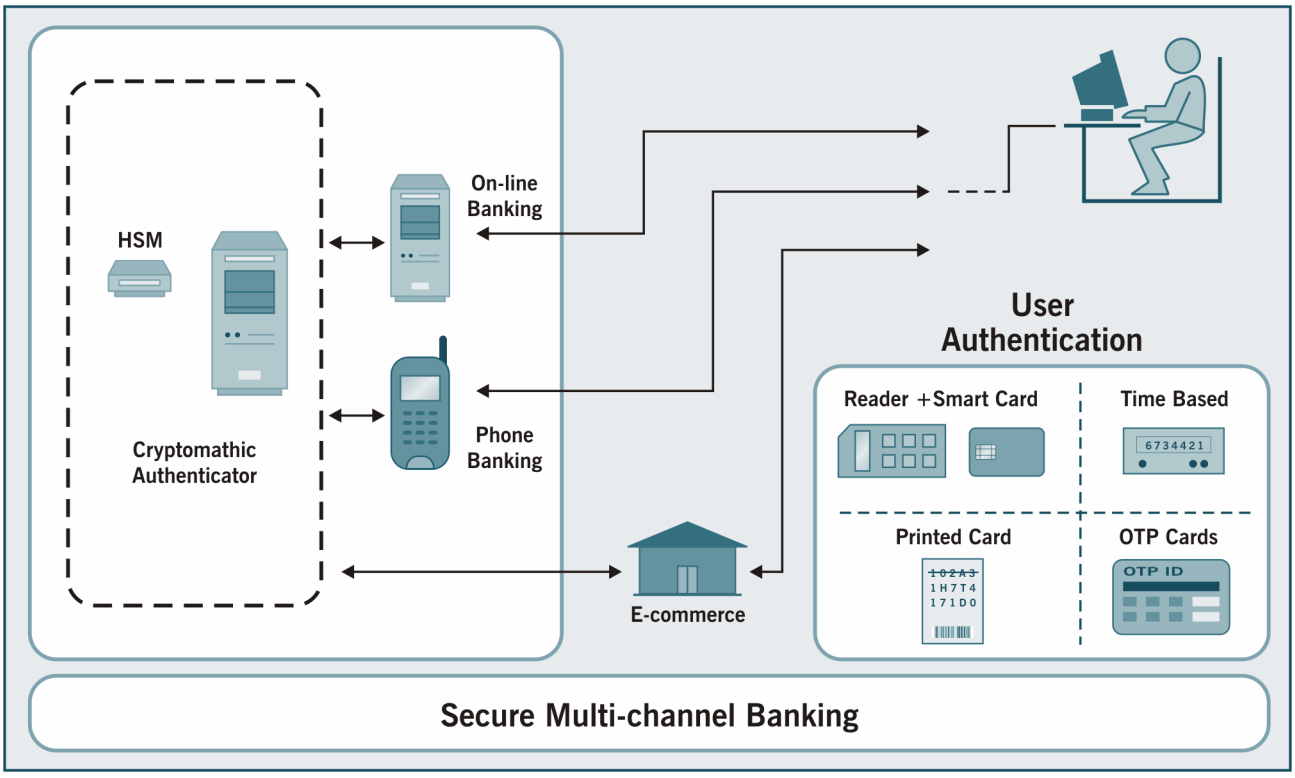

Figure 1 – The Cryptomathic Authenticator Service Delivery Model

As already identified, Cryptomathic Authenticator supports multiple authentication mechanisms, tokens, and smart cards etc., and through the use of its best-practice key management facilities, provides security for banking customers against external and internal attacks.

By definition, strong authentication dictates that more than just a static password is used to confirm the access credentials of a customer. Typically, it requires a two-from-three approach, where the options available include:

1. Something the customer has – a one shot token for example.
2. Something the customer knows – a password perhaps.
3. Something that the customer is – could be a biometric signature.

For bank customers, the biometric option appears to be the least practical, leaving additional token or smartcard authentication approaches as the most manageable and workable way forward. Using such approaches customers would present their normal on-line credentials, and then add the information from a unique one-time token-based cryptographic key. At the systems end the Cryptomathic Authenticator maintains a copy of each customer's credentials and uses these to authenticate the access request.

In operational use to maintain this level of security, each time a customer wishes to access their on-line banking facilities they are presented with a log-on page from the bank's Web access control system. The customer then enters their on-line banking customer ID, together with a static password, and the one-time key generated by their token.

The customer ID, static password, and one-time key are received by the bank's Web access control system, which then validates the things that it knows about the customer and their sign on credentials. If these checks are successfully completed, the banks Web access control system then accesses the customer database to map the customer ID to the token ID, and calls the Cryptomathic Authenticator passing on the token's own unique identity and the one-time key that is being used.

The Cryptomathic Authenticator responds by using its databases to look up the customer keys for that particular token ID, and then calls the HSM to process the request and validate the one-time key that has been presented. To complete the process, the response from the HSM of 'Yes access is allowed' or 'No access is denied' is passed back to the bank's Web access control system by the Cryptomathic Authentication server.

Each generated key is received by the Cryptomathic Authenticator system on a one-time basis. Operationally this means that the same code cannot be used again to authenticate systems access, and most importantly, even if the code was intercepted or given out freely by a customer to a third party it could not be reused. Under such circumstances, threats from Trojan, Spyware, and key logger attacks, where a virus or program installs itself in a customer's PC, reporting back on banking and password details; Phishing and Pharming attacks where fraudsters try to trick customers into revealing password details; Man-in-the-Middle attacks where information is intercepted whilst the customer is on-line; and Insider Attacks where a bank employee exploits the security system 'in-house' can all be massively reduced, or eradicated.

The processes described in this section of the Technology Audit are valid for on-line banking customers, and can also provide similar authentication-controls for phone-based access to banking systems and for customer-not-present e-commerce transactions, where the authentication of a sale can be validated through the use of one-time tokens.

Product Emphasis

Most of us make regular use of the Internet as a source of information for business and personal requirements. In this context it is an extremely open, flexible, and available medium. Where we have reservations over its future use are in areas such as on-line banking and transacting payments in a retail environment, areas where direct access is required to personal and financial information. To date the financial services industry has been slow to allay our fears about information theft, or indeed to take proactive action in this area. As a result, Phishing, Spyware, and associated attacks on personal and financial details have flourished, and the banks should now be becoming seriously concerned that the continued open use of such cost-efficient, self-service access channels will be adversely affected.

Cryptomathic Authenticator from Cryptomathic Ltd. delivers a dual value proposition. For financial institutions it provides a proven, secure, and cost-efficient authentication vehicle that can be deployed without disrupting existing banking and customer management systems. For customers it provides the ability to deliver a secure, easy to use, one-time authentication methodology that cannot be freely or accidentally undermined by malicious identity theft activities.

▶ DEPLOYMENT

The Cryptomathic Authenticator solution is normally deployed in-line and alongside a financial organisation's own legacy systems, in order to deliver an extra layer of customer authentication, although where required it can also operate independently. At its point of deployment the solution requires the availability of a range of basic systems and server management and installation skills. These include some knowledge of HTTP to cover basic integration requirements, and integration with management interfaces, which may be optional in some installations. It also requires a level of expertise in the use of Web services and SOAP.

Installers need to have a working understanding of standard operational systems concepts, and administration and set up elements need to be supported by a good knowledge of industry standard security principles. In addition, some database management knowledge is required which, dependant upon systems complexity, can range from basic installation and administration skills, up to expert database knowledge to deal with clustering, hot failover, and real-time backup requirements. Deployment timescales are driven by systems complexity issues, but can start from as little as two hours for the installation and integration of a very basic system with no customer management requirements.

Following installation very little in the way of systems administration should be required. Even where the system has been deployed alongside, and integrated with, an organisation's customer management system normal token management and customer management activities are external to the Cryptomathic solution being delivered through standard back-office systems channels.

Cryptomathic provides training that covers the requirements of systems integrators (rarely requested), systems administrators, company auditors, and systems administrators. Such training can be provided on the customer's site and is supported by a comprehensive range of integration, installation, administration, and maintenance manuals. Systems support and maintenance is also provided by Cryptomathic, and is available on a level to suit the needs of the customer – weekday office hours, weekday 24-hour, and on a 24x7 cover.

The main platform that is used when deploying Cryptomathic Authenticator is currently Microsoft Windows Server 2003, although the product can be ported to various UNIX platforms if required. The system operating framework is Microsoft NET, and the supporting databases can be run on either Microsoft SQL or Oracle platforms. HSMs supported include: nCipher and Eracom. Other additional requirements may include the use of smartcard readers (normally GEMplus), and a systems toolkit for the integration of certain cryptographic functions.

Once deployed some changes will need to be made to operational procedures within the end-user organisation as Cryptomathic Authenticator adds an additional layer of security. However, this should have only a very small impact on day-to-day operations and the main changes will be seen by the organisation's customers, who may be asked to use one-time authentication tokens or smartcards each time they sign in to the system.

The standard Cryptomathic Authenticator solution normally includes an authentication server and database, with one or more HSM and smartcard readers attached. Some form of authentication tokens or smartcards will be required to drive user authentication, but their selection and deployment is seen as external to the core system.

▶ PRODUCT STRATEGY

The target market for Cryptomathic Authenticator is small, medium, and large banks, and financial institutions that provide their customers with self-service, Internet, and telephone access to account and financial information. Return on Investment is said by Cryptomathic to be 100% after one year for a full roll-out. The calculation is based on comparing systems costs incurred by the authenticator system against the fraud overheads that its deployment is able to eliminate. In addition, a further argument in favour of the solution is that it encourages customers to continue to use cost effective, on-line, self-service facilities, rather than reverting to other more expensive communications channels.

In the UK, Lloyds TSB has just announced the trial of a new security system for Internet banking. Based on two-factor authentication; each customer involved (30,000) will receive a key-ring token security device, which generates a six-digit code to be used alongside their username and password. The technology that is being used to deliver centralised authentication services for every access request is Cryptomathic Authenticator. The HSM component of the solution's authentication engine is being provided by nCipher Ltd, one of Cryptomathic's preferred technology partners.

Because Cryptomathic Authenticator supports a wide range of authentication schemes, it avoids both technology-mandated solutions and vendor lock-in to a particular authentication scheme. The product is brought to market via reseller and partner channels. Key business partners and technology partners include: nCipher, Eracom, Vasco, Xiring, Mastercard, and Visa.

For each deployment there is a one-off licensing cost, this is based on the number of potential users, and the organisations requirements for fail-over, redundancy, and scalability etc. Annual support costs are based on the company's three-tier support infrastructure (weekday office hours, weekday 24 hour, and 24x7 cover). Typical project costs are difficult to quantify, but may be as wide ranging as UK£20,000 to over UK£1 million. Major systems releases, that are covered by the systems maintenance contract, are made on a bi-annual basis.

▶ COMPANY PROFILE

Cryptomathic was founded as a university spin off back in 1986 by Professor Peter Landrock. The company, which remains in private ownership, has its headquarters in Aarhus, Denmark, and also has major offices in Munich, Germany, and Cambridge in the UK. Cryptomathic is known as a leading provider of strong security solutions that are used across a wide range of business and industry sectors including: finance and banking, government, and the digital rights management and smart card sectors. The company prides itself on its strength of technical expertise employing some of the world's leading cryptographers, including Vincent Rijmen and Ivan Damgaard.

Today the company employs around 60 staff across its European operations, and with more than 50% employed in Research and Development (R&D) activities, it continues to focus on the development and provision of industry focused, high-quality protection solutions.

As a privately held security company Cryptomathic does not make public either its revenue figures or its list of existing customers. However, it was prepared to confirm that its revenue split by region was US 30%, Europe 55%, Asia 5%, Middle East 5%, and elsewhere 5%, and that its customer base, across the company's product portfolio, extends to hundreds of customers, and that five of these are already using its new Cryptomathic Authenticator product.

▶ SUMMARY

In the banking sector, delivering secure on-line customer protection services that cannot be compromised by Phishing, Pharming, Spyware, Trojans, or any other form of information theft, has proved to be a significant stumbling block. Variations on fixed password approaches have been tried, but customers can still be fooled into making this type of static information available to malicious third parties, and as a result, leave themselves open to having their accounts fraudulently attacked. Therefore, in Butler Group's opinion, for those financial institutions that are looking to maintain or further increase the use of this cost-efficient, self-service, customer access channel, it is time to take more effective action.

In the UK, customer trials using the Cryptomathic Authenticator solution to provide secure, central-server, one-time customer authentication services, are currently being carried out by Lloyds TSB. Butler Group believes that this represents a major step forward in the way that on-line customers are being valued and, assuming that the use of the systems one-time tokens proves popular with its customers, it should result in increased on-line account usage for that bank.

Furthermore, should the trial prove to be a success, we would expect to see other mainstream banks and building societies formulating their own enhanced on-line customer protection/authentication strategies. Under these circumstances, Cryptomathic, with its Cryptomathic Authenticator solution, would be strongly positioned as a proven supplier of key authentication services.

Contact Details

Headquarters
CRYPTOMAThIC A/S
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark

Tel: +45 8676 2288
Fax: +45 8620 2975

www.cryptomathic.com

UK/Ireland
CRYPTOMAThIC Ltd
329 Cambridge Science Park, Milton Road
Cambridge, CB4 0WG
UK

Tel: +44 (0)1223 225350
Fax: +44 (0)1223 225351

Butler Group
a Datamonitor Company

Headquarters:

Europa House,
184 Ferensway,
Hull, East Yorkshire,
HU1 3UT, UK

Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Australian Sales Office:

Butler Direct Pty Ltd., Level 21,
Tower 2, Darling Park,
201 Sussex Street,
Sydney NSW 2000, Australia

Tel: + 61 (0)2 9955 6249
Fax: + 61 (0)2 9006 1282

End User Sales Office (USA):

Butler Group,
245 Fifth Avenue, 4th Floor,
New York, NY 10016,
USA

Tel: +1 212 652 5302
Fax: +1 212 686 2626

For more information on Butler Group's Subscription Services please contact one of the local offices above.